Information Security Maturity Model for NIST Cyber Security Framework

Sultan Almuhammadi and Majeed Alsaleh

College of Computer Sciences and Engineering,
King Fahd University of Petroleum and Minerals,
Dhahran, Saudi Arabia
Emails: muhamadi@kfupm.edu.sa, g198925300@kfupm.edu.sa

Abstract

The National Institute of Standards and Technology (NIST) has issued a framework to provide guidance for organizations within critical infrastructure sectors to reduce the risk associated with cyber security. The framework is called NIST Cyber Security Framework for Critical Infrastructure (CSF). Many organizations are currently implementing or aligned to different information security frameworks. The implementation of NIST CSF needs to be aligned with and complement the existing frameworks. NIST states that the NIST CSF is not a maturity framework. Therefore, there is a need to adopt an existing maturity model or create one to have a common way to measure the CSF implementation progress. This paper explores the applicability of number of maturity models to be used as a measure to the security poster of organizations implementing the NIST CSF. This paper reviews the NIST CSF and compares it to other information security related frameworks such as COBIT, ISO/IEC 27001 and the ISF Standard of Good Practice (SoGP) for Information Security. We propose a new information security maturity model (ISMM) that fills the gap in the NIST CSF.

Keywords

Information Security, Maturity Model, Cyber-Security.

1. Introduction

Many organizations could be aligned with one of the information security related best practice frameworks. This makes the alignment of the NIST CSF with such frameworks a must. NIST CSF is a set of industry standards and best practices [1]. The framework of NIST CSF clearly indicates that organizations planning to implement it can use their existing processes and place them on top of the NIST CSF to identify gaps with respect to the framework. This implies the comprehensiveness of the NIST CSF when compared with other frameworks such as COBIT, ISO/IEC 27001 and ISF Standard of Good Practices (SoGP). Thus, to ensure applicable alignment with any information security framework, we need to confirm the comprehensiveness or identify any possible gap in NIST CSF.

However, in this paper, we show that NIST CSF is not comprehensive to address all information security related processes that are addressed in some of those frameworks. The main objective of the framework is to manage cyber security risks within the organizations that implement it. In the NIST CSF, the "Framework Implementation Tiers" part, referred to as "Tiers", is detailed as one of three parts that the framework consists of [1]. However, the Tiers does not provide organizations with a mechanism to measure the progress of implementing NIST CSF or their maturity level and information security processes' capabilities. Tiers is just visionary tool that allows organizations to understand

their cyber security risk management approach and what are the processes in place to manage the risk. NIST official web site [2] has stated that the Tiers are not intended to be measurement tool to maturity levels.

This paper is a comprehensive comparison between NIST CSF, COBIT, ISO/IEC 27001 and ISF frameworks. It identifies the gap of key information security processes that are addressed in some frameworks but not in NIST CSF. We fill this gap and propose a new capability maturity model (CMM) to measure NIST CSF implementation progress.

2. Overview of the NIST Cyber Security Framework

The NIST CSF consists of three main parts in which, cyber security is considered as a risk that is managed through the enterprise risk management process [1]. Thus, we identify the NIST CSF framework as risk-based framework. The three parts are: framework core, risk tiers, and framework profile.

Table 1: Frameworks Comparison

Framework	Control Categories	Control Objectives	Activities
NIST CSF [1]	Functions (5)	Categories (22)	Subcategories (98)
ISF [3]	Categories (4)	Areas (26)	Topics (118)
ISO27001 (2013) [4]	Clauses (14)	Control objective(35)	Controls (114)
COBIT5 (2013) [5]	Domains (5)	Processes (37)	Practices (210)

2.1. Framework Core

The framework core consists of a set of cyber security activities. These activities are grouped in "Subcategories" which are grouped too in "Categories". The categories are sorted in five different "Functions": Identify, Protect, Detect, Respond, and Recover. The NIST CSF five functions are concurrent and continuous. When the functions collectively implemented they form a high-level and strategic view of the cyber security risk management program. The Framework Core part has also the desired outcomes (controls objectives) and informative references. Informative references are list of cyber security activities in standards, guidelines, or practices such as as COBIT, ISO/IEC 27001 and the ISF SoGP. The comparison between the NIST CSF and other frameworks will be done on the level of the cyber security activities to ensure that all key information securities activities are addressed. Table 1 compares the structure of NIST CSF with the structure of selected sample of frameworks.

2.2. Risk Tiers

The Tiers part of the NIST CSF is a visionary tool that allows organizations to understand their cyber security risk management approach and what are the processes in place to manage the risk. Based on the identified processes in place, the organization may be classified in one of four tier levels. The tier levels range from "Partial" in Tier 1,"Risk Informed" in Tier 2, "Repeatable" in Tier 3, to "Adaptive" in Tier 4.

2.3. Framework Profile

The framework profile, referred to as "profile", is a tool to document, implement, and track the organizations' opportunities for improving their cyber security posture. The profile has the current cyber security activities implemented by the organization, as well

as the planned activities to be implemented in order to close the gap between the current and the "to-be" state. Organizations need to identify which cyber security activities are needed to improve the current state based on risk assessment to identify risks that may prevent achieving the business objectives.

3. Related Work

We reviewed the "Baldrige Excellence Framework" and "Baldrige Excellence Builder" at NIST website [6]. We found that these two documents were not introduced to serve as Maturity Model. However, they are a continues effort linked to the Tiers, where the main aim is to help organizations to evaluate how effective is their cyber security risk management effort. The Baldrige Excellence Builder links the cyber security program with several areas such as leadership, customers, employees, and the outcome results. In [7], the authors proposed a method to select measures which evaluate the gap between the current and the target states based on the NIST CSF risk Tiers. In [8], on the other hand, the authors highlighted the need for Compliance Assessment in order to reduce the gap in the Processes pillar (one of three pillars including Human Resources and Technology). Therefore, they proposed a model that is generic to allow for overall compliance evaluation.

4. NIST CSF Evaluation

NIST CSF, as a framework, has the following nature:

- Focus on information security high-level requirements.
- Applicable for the development of information security program and policy

Examples of other frameworks include, COBIT, ISO/IEC 27001 and the ISF SoGP for Information Security. However, the detailed cyber security activities are usually listed in standards, guidelines, and practices. They have the following nature:

- Focus on information security technical and functional controls (customizable).
- Applicable for developing checklists and conducting compliance/audit assessments.

Examples of standards and guidelines include NIST SP 800-53, ISO-27001 Annex, and ISF SoGP. The NIST CSF has mapped number of standards in the informative references. The mapped standards include NIST SP 800 series, COBIT 5, ISA 62443, ISO/IEC 27001:2013, and CCS [1]. ISF SoGP was not mapped in the NIST CSF framework. Therefore, we will use the ISF SoGP mapping [9] to NIST CSF to conduct the comparison with NIST CSF.

NIST CSF clearly indicates that organizations planning to implement it can use their existing processes and place them on top of the NIST CSF to identify gaps with respect to the framework [1]. However, this assumes that NIST CSF will be comprehensive and adopted framework will be always equal or less than NIST. This is illustrated in Figure 1-a.

Of course the other scenario of NIST CSF being not comprehensive and has a gap when compared with other frameworks is possible. In order to verify this scenario (illustrated in Figure 1-b), we matched all mapped CSF informative references with the corresponding framework. Numeric statistics of this match are as follows:

Framework	CSF	Gap	Gap %
ISO 27001	93	21	18.4%
ISF	49	69	58.5%
COBIT5	165	45	21.4%

We found that the compliance process is one gap area, related to information security, that is identified and need to be addressed in future update to NIST CSF. For example, MEA03

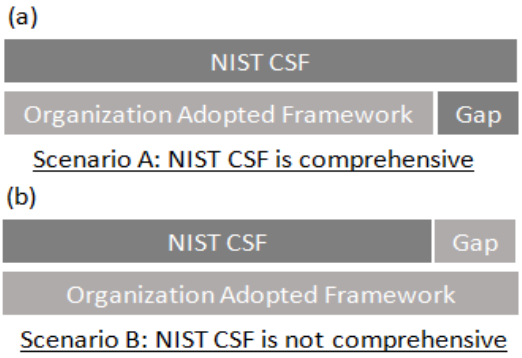

Figure 1: Two gap scenarios for CSF being comprehensive

(Monitor, Evaluate and Assess Compliance with External Requirements) is a COBIT process that is not mapped to NIST CSF. Also, SI2.3 (Monitoring Information Security Compliance) is ISF process that is not mapped to NIST CSF. In addition, ISO/IEC 27001 has one process (A.18: Compliance) that is partially mapped to NIST CSF. NIST CSF has mapped only the following five ISO/IEC processes: A.18.1 (Compliance with legal and contractual requirements), A.18.1.3 (Protection of records), A.18.1.4 (Privacy and protection of personally identifiable information), A.18.2.2 (Compliance with security policies and standards), and A.18.2.3 (Technical compliance review).

We traced the Compliance Assessment in NIST 800 series and found two main publications ([10] and [11]) that highlighted this topic. The Compliance Assessment was addressed under the Risk Monitoring process, roles and responsibilities associated with it. The two main objectives of the Risk Monitoring process are to verify the existence of the control (Compliance) and the efficiency of the control to mitigate the risk [11]. Compliance assessment is very essential to ensure that identified control to mitigate the risk is implemented correctly and operating as intended. For detailed responsibilities of each role in the compliance process refer to the following in [10]:

Role	Reference [10]
Info. system owner	Sec. D.9, Page D-5
Info. system security officer	Sec. D.10, Page D-6
info. security architect	sec. D.11, Page D-6
security control assessor	sec. D.13, Page D-7

We propose to add the compliance assessment process as a process in NIST CSF (be the category number 23). This category will contain the missed subcategories highlighted previously. The process should at least contain the following as subcategories:

- Legal and Regulatory Compliance
- Information Privacy
- Intellectual property
- Compliance with security policies and standards

5. Measuring Maturity of Organizations Implementing NIST CSF

The profile part of the NIST CSF is focused on tracking the organization progress in implementing the gaps to move from the current state to the defined target. NIST CSF has provided the Tiers as visionary tool that allows organizations to understand their cyber security risk characteristics. However, as we highlighted in Section 1, Tiers does not

provide organizations with a mechanism to measure the progress of implementing NIST CSF or their maturity level and information security processes capabilities.

Therefore, a maturity model is needed to measure the information security processes capabilities. The main objective of such maturity model is to identify a baseline to start improving the security posture of an organization when implementing NIST CSF. The maturity model then is used in cycles to build consensus, set the priorities of investment in information security, and after all measure the implementation progress [12]. Some of the frameworks that we studied come with maturity model (like COBIT and ISF). For other frameworks that do not have maturity model like ISO 27001, other information security related maturity models like ONG C2M2 and SSE MM are used (Figurs 2 and 3). We studied the different maturity models to verify if they map to each other in order to utilize any of them to measure the maturity of organizations implementing NIST CSF. The main focus of our study was to compare the scale used by each model and the domains evaluated by each model.

We reviewed the four maturity models SSE CMM [13], ONG C2M2 [14], ISF MM [15], and COBIT PAM MM [16]. Unlike the other three maturity models, ONG C2M2 is three scale model and assesses ten domains. Refer to Figure 2.

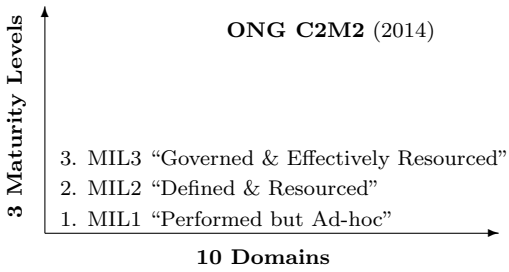

Figure 2: ONG C2M2 Maturity Model scales and domains

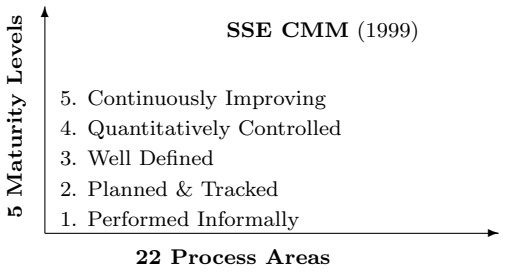

Figure 3: SSE Maturity Model scales and domains

While SSE CMM (Figure 3), ISF MM (Figure 4) and PAM MM (Figure 5) are the same scale maturity models, yet the problem of mapping exists. In Table 2, we identified that level 2 "Planned and Tracked" of SSE CMM is not mapped to any of the other maturity models. Figure 3 illustrates the levels and domains of SSE CMM. On the other hand, in ISF MM and PAM MM, level 2 and 3 is the opesite of each other. Figures 4 and 5 illustrate the levels and domains of ISF MM and PAM MM.

We performed a comprehensive comparison of all the domains in the four maturity models. These domains are carefully examined in an attempt to verify the applicability of any

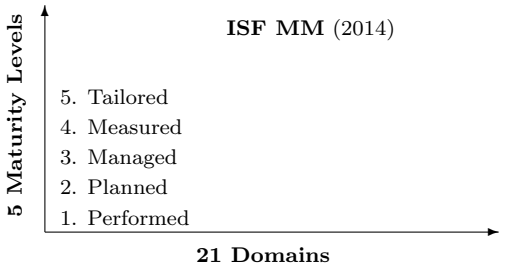

Figure 4: ISF Maturity Model scales and domains

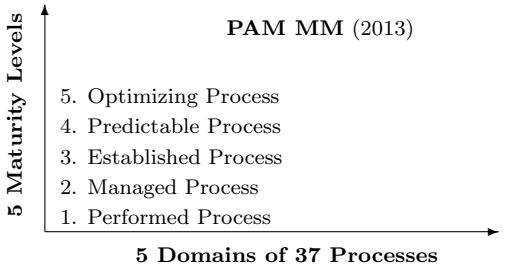

Figure 5: PAM Maturity Model scales and domains

Table 2: Maturity Models Scale Comparison

SSE CMM [13]	ISF MM [15]	COBIT PAM [16]	ONG C2M2 [14]
L1 Performed Informally	L1 Performed	L1 Performed Process	L1 Performed but Ad-hoc
L2 Planned and Tracked	No Mapping	No Mapping	No Mapping
L3 Well Defined	L2 Planned	L3 Established Process	L2 Defined and Resourced
No Mapping	L3 Managed	L2 Managed Process	L3 Governed and Effectively Resourced
L4 Quantitatively Controlled	L4 Measured	L4 Predictable Process	No Mapping
L5 Tailored	L5 Continuously Improving	L5 Optimizing Process	No Mapping

maturity model regardless of the deployed framework. However, our study shows the lack of one-to-one mapping or any clear way to map these domains in an applicable way. There are items in certain models that are mapped to multiple items in other models. While other items have no mapping as show in Table 3. For example, "Monitor Posture" in SSE CMM is mapped to three items in ISF MM, three items in PAM, and two items in ONG C2M2. While "Monitor and Control Technical Effort" in SSE CMM and "Manage Operation" in PAM have no mapping in ISF MM and ONG C2M2. Moreover, the "Administer Security Controls" in SSE MM is mapped to seven items in PAM MM.

Our study, as summarized in Tables 2 and 3, illustrates the mapping of ONG C2M2 with the other three maturity models in Table 2. It shows that ONG C2M2 has similarity and map to the first three levels of the ISF MM (Figure 4). However, there is a gap in the assessed areas due to the difference in the number of both maturity models (10 assessed areas in ONG C2M2 versus 21 in ISF MM). There are assessed areas in ISF MM which are not mapped to ONG C2M2 such as "Compliance", "Security Audit", "Security Architec-

Table 3: Maturity Models Domains Comparison

SSE CMM [13]	**ISF MM [15]**	**COBIT PAM [16]**	**ONG C2M2 [14]**
No Mapping	Security Strategy	Manage Strategy	Cybersecurity Program Management
Administer Security Controls*	Security Governance	Ensure Governance Framework Setting and Maintenance	
		Ensure Benefits Delivery	
		Ensure Risk Optimization	
		Ensure Resource Optimization	
		Ensure Stakeholder Transparency	
Specify Security Needs	Security Policy	Manage the IT Management Framework	
Assess Security Risks	Information Risk Management	Manage Risk	Risk Management
Manage Project Risk			
Assess Threats			
Assess Impact			
Verify and Validate Security	Compliance	Monitor, Evaluate and Assess Performance and Conformance	No Mapping
Build Assurance Augment		Monitor, Evaluate and Assess the System of Internal Control	
		Monitor, Evaluate and Assess Compliance ...	
	Security Audit		No Mapping
Administer Security Controls*	Asset Management	Manage Assets	Asset, Change, and Configuration Management
Manage Configuration	Change Management	Manage Configuration	
		Manage Change	
		Manage Organizational Change Ennoblement	
		Manage Change Acceptance and Transitioning	
No Mapping	Identity and Access Management	Manage Security Services	Identity and Access Management
Assess Vulnerabilities	Vulnerability Management		Threat and Vulnerability Management
Monitor Posture	Threat Intelligence		
	Security Event Management	Manage Service Requests and Incidents	Event and Incident Response, Continuity of Operations
	Incident Management	Manage Problems	
No Mapping	Business Continuity	Manage Continuity	
No Mapping	Crisis Management		
Coordinate Security	No Mapping	Manage Security	No Mapping
Plan Technical Effort	No Mapping	Manage Programs and Projects	No Mapping
		Manage Portfolio	
		Manage Budget and Costs	
Monitor and Control Technical Effort	No Mapping	Manage Operations	No Mapping
Provide Security Input	Security Architecture	Manage Enterprise Architecture	No Mapping
Define Organization Systems Process		Manage Requirements Definition	
Improve Organization Systems Engineering Process		Manage Solutions Identification and Build	
Manage Systems Engineering Support Environment		Manage Availability and Capacity	
Manage Product Line Evolution		Manage Innovation	
Ensure Quality	Secure Application Development	Manage Quality	No Mapping
No Mapping	Digital Connections	Manage Assets*	Information Sharing and Communications
Provide On-Going Skills	Human Resources Security	Manage Knowledge	Workforce Management
		Manage Human Resources	
Administer Security Controls*	Security Awareness and Behavior	Manage Security*	Situational Awareness
Coordinate with Suppliers	External Supplier Management	Manage Relationships	Supply Chain and External Dependencies Management
		Manage Service Agreements	
		Manage Suppliers	
No Mapping	No Mapping	Manage Business Process Controls	No Mapping

* This item is mapped to multiple items in other models

ture", and "Secure Application Development". Other areas of ONG C2M2 are mapped to more than one area in ISF MM. For example, "Cyber security Program Management" in ONG C2M2 was mapped to three areas in ISF MM, namely,"Security Strategy", "Security Governance", and "Security Policy".

6. Proposed Information Security Maturity Model

In the previous sections, we discussed few critical issues about NIST CSF framework. In order to understand the importance of a new cabability maturity modle for the NIST CSF, we highlight the following factors:

- The need for business management to measure the maturity of the security program to assure the reliability of the IT services enabling and supporting their business [12].
- NIST CSF framework tiers are not intended to be measurement tool to maturity levels [2].
- The identified gap in NIST CSF.
- The lack of (one-to-one) mapping in both scale levels and the assessed areas of the different existing maturity modules.

Taking into considerations all the above factors, there is a need to define a new CMM for NIST CSF. Therefore, we propose a five-level scale with 23 assessed areas as shown in Figure 6. Our suggested assessed areas are shown in Table 4. These areas are the 22 in NIST CSF categories plus the compliance assessment (No. 6 in Table 4).

Table 4: The 23 assessed areas of the proposed maturity model

1	Asset Management
2	Business Environment
3	Governance
4	Risk Assessment
5	Risk Management Strategy
6	Compliance Assessment*
7	Access Control
8	Awareness and Training
9	Data Security
10	Information Protection Processes and Procedures
11	Maintenance
12	Protective Technology
13	Anomalies and Events
14	Security Continuous Monitoring
15	Detection Processes
16	Response Planning
17	Response Communications
18	Response Analysis
19	Response Mitigation
20	Response Improvements
21	Recovery Planning
22	Recovery Improvements
23	Recovery Communications

* Not addressed in any of the NIST CSF 22 Categories

Three of the four maturity models we compared are five-level scales in addition of other five information security related maturity models reviewed by [12]. This supports our

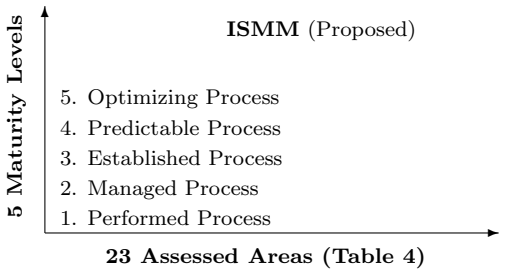

Figure 6: Proposed Information Security Maturity Model (ISMM)

decision to make the proposed maturity model a five-level scale. However, detailed review of the required scale characteristics, such as the scale levels, scale level definitions, or scale measures (staged versus continuous), need to be addressed in future work.

The proposed ISMM will enable the organizations to measure their implementation progress over time. They will use the same measuring tool in a regular basis to ensure maintaining the desired security posture. Furthermore, using the same measuring tool by different organizations will allow the benchmarking between those organizations [12].

7. Conclusion

NIST CSF has been introduced to organizations with critical infrastructure as an integrated framework to implement in order to improve their security postures. The NIST recommended to use the framework on top of and to complement any implemented framework within the organization. The ongoing enhancement nature of the information security programs drives the organizations to continuously measure their capabilities of achieving the desired outcome of the implemented framework. The organizations use the capability maturity models to evaluate their capabilities. This will give the management of the organization the bases of their decisions to define and prioritize their investment strategy in building the information security.

This paper considered the evaluation of the NIST CSF comprehensiveness to ensure that it will cover any existing framework. Moreover, the paper reviewed number of maturity models to assess the applicability to use with NIST CSF and the existence of mapping between the NIST CSF control objectives and the assessed areas. The paper used three information security related frameworks (ISO 27001, ISF, and COBIT5) and four maturity models (ISF, PAM, SSE CMM, and ONG C2M2).

The review considered the mapping made by NIST CSF to other frameworks and confirmed that the NIST CSF did not adequately address the compliance assessment process. The evaluation of the maturity models considered the scale levels definitions and the assessed areas. In both dimensions, there was no one-to-one mapping between the different maturity models. Therefore, we concluded that none of the evaluated maturity models can be used with NIST CSF to have a wide coverage and mapping to implemented framework. The paper proposed a new maturity model of five-level scale and include the twenty two NISCT CSF categories with addition of the compliance assessment process.

As for the future work, first, this paper shows the comparison between the assessed areas in different maturity models, but it did not compare them with the NIST CSF. This comparison is important to identify which maturity model can be used as a bases to define the scale levels of the proposed NIST CSF maturity model. The scope of the comparison also needs to be expanded to cover more cyber security and information security related

maturity models such as the Community Cyber Security Maturity Model [17] and the Information Security Governance model [12]. Second, the current best practice of the information security business structure needs to be considered to resort the 23 assessed areas according to that structure grouping areas performed in one entity together. For example, business processes like the asset management, change management, threat monitoring, or risk management might be used to group related NIST CSF categories.

8. References

[1] NIST, "Framework for improving critical infrastructure cybersecurity," http://www.nist.gov/cyberframework/upload/cybersecurity-framework-021214.pdf, 2014.

[2] N. Keller, "Cybersecurity framework faqs framework components," https://www.nist.gov/cyberframework/cybersecurity-framework-faqs-framework-components, 2015, accessed: December 11, 2016.

[3] ISF, "The standard of good practices for information security," in *Information Security Forum ISF*, 2014.

[4] S. Schweizerische, "Information technology-security techniques-information security management systems-requirements," *ISO/IEC International Standards Organization*, 2013.

[5] ISACA, "Cobit 5: A business framework for the governance and management of enterprise it," 2012.

[6] L. Scott, "Baldrige cybersecurity initiative," https://www.nist.gov/baldrige/products-services/baldrige-cybersecurity-initiative, 2016, accessed: November 10, 2016.

[7] S. Fukushima and R. Sasaki, "Application and evaluation of method for establishing consensus on measures based on cybersecurity framework," in *The Third International Conference on Digital Security and Forensics (DigitalSec2016)*, 2016, p. 27.

[8] N. Teodoro, L. Gonçalves, and C. Serrão, "Nist cybersecurity framework compliance: A generic model for dynamic assessment and predictive requirements," in *Trustcom/BigDataSE/ISPA, 2015 IEEE*, vol. 1. IEEE, 2015, pp. 418–425.

[9] ISF, "Isf standard and nist framework poster," in *Information Security Forum ISF*, 2014.

[10] J. T. FORCE and T. INITIATIVE, "Guide for applying the risk management framework to federal information systems," *NIST special publication*, vol. 800, p. 37, 2010.

[11] P. D. Gallagher and G. Locke, "Managing information security risk organization, mission, and information system view," *National Institute of Standards and Technology*, 2011.

[12] M. Lessing, "Best practices show the way to information security maturity," http://hdl.handle.net/10204/3156, 2008, accessed: January 10, 2017.

[13] Carnegie-Mellon-University, "Systems security engineering capability maturity model (sse-cmm) model description document version 3.0," 1999.

[14] D. of Energy, "Oil and natural gas subsector cybersecurity capability maturity model (ong-c2m2 v1.1)," *Department of Energy, Washington, DC: US*, 2014.

[15] ISF, "Time to grow using maturity models to create and protect value," in *Information Security Forum ISF*, 2014.

[16] ISACA, *COBIT Process Assessment Model (PAM): Using COBIT 5.* ISACA, 2013.

[17] G. B. White, "The community cyber security maturity model," in *Technologies for Homeland Security (HST), 2011 IEEE International Conference on.* IEEE, 2011, pp. 173–178.